PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-312317
(43)Date of publication of application : 25.10.2002

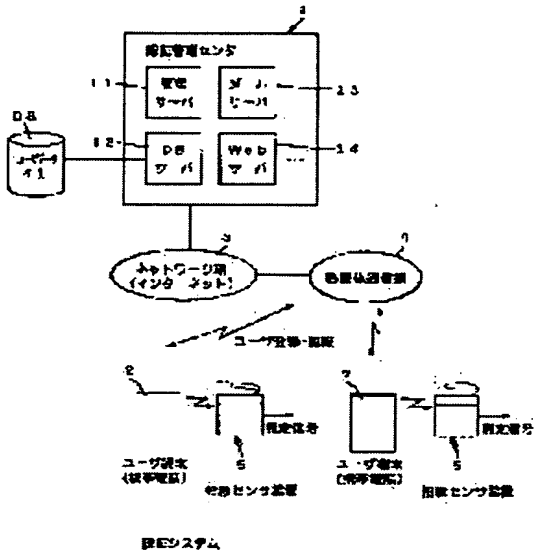
(51)Int.Cl. G06F 15/00
H04L 9/08
H04L 9/32

(21)Application number : 2001-112740
(22)Date of filing : 11.04.2001

(71)Applicant : CASIO COMPUT CO LTD
(72)Inventor : AKAO HIDETOSHI

(54) CERTIFICATION SYSTEM AND CERTIFICATION METHOD

(57)Abstract:
PROBLEM TO BE SOLVED: To realize a certain security management capable of effectively protecting a user certification information by dividing the user certification information for a setting registration to a plurality of constitution elements and dispersely managing them.
SOLUTION: A certification management center 1 divides the user certification information sent from a fingerprint sensor device 5 through a user terminal 2 at the time of registration of the user and allots one constitution element of respective constitution elements of the user certification information divided to a registration information at a system side and the other constitution element to a registration information set in the user terminal 2. The registration information in the user terminal 2 is obtained and the registration information at the system side is obtained from a user data base DB at the time of certification of the user. After the original user certification information is produced and restored based on the registration information in the user terminal 2 and the registration information at the system side obtained, the user certification is carried out by comparing the user certification information restored with the user certification information inputted at the time of certification of the user.



LEGAL STATUS

[Date of request for examination] 23.08.2004
[Date of sending the examiner's decision of rejection]
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
[Date of final disposal for application]
[Patent number]
[Date of registration]
[Number of appeal against examiner's decision of rejection]
[Date of requesting appeal against examiner's decision of rejection]
[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2002－312317
（P2002－312317A）
(43)公開日　平成14年10月25日(2002.10.25)

(51)Int.Cl.[7]	識別記号	ＦＩ	テーマコード（参考）
Ｇ０６Ｆ　15/00	３３０	Ｇ０６Ｆ　15/00	３３０Ｂ　５Ｂ０８５
			３３０Ｆ　５Ｊ１０４
Ｈ０４Ｌ　9/08		Ｈ０４Ｌ　9/00	６７３Ｚ
9/32			６７３Ｄ
			６７５Ｄ

審査請求　未請求　請求項の数８　ＯＬ　（全 11 頁）　最終頁に続く

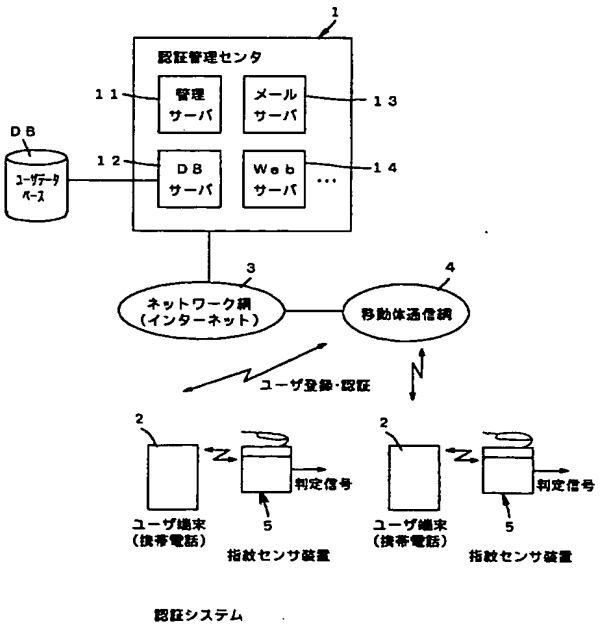
(21)出願番号　特願2001－112740(P2001－112740)
(22)出願日　平成13年４月11日(2001.4.11)

(71)出願人　000001443
カシオ計算機株式会社
東京都渋谷区本町１丁目６番２号
(72)発明者　赤尾　英俊
東京都羽村市栄町３丁目２番１号　カシオ計算機株式会社羽村技術センター内
(74)代理人　100073221
弁理士　花輪　義男

Ｆターム(参考)　5B085 AA08 AE26 BA07
5J104 AA08 EA03 EA13 KA01 MA01
NA05

(54)【発明の名称】　認証システムおよび認証方法

(57)【要約】
【課題】設定登録用のユーザ認証情報を複数の構成要素に分割して分散管理することで、そのユーザ認証情報を効果的に保護することができる確実なセキュリティ管理を実現できるようにする。
【解決手段】認証管理センタ１は、ユーザ登録時に、指紋センサ装置５からユーザ端末２を介して通信されて来たユーザ認証情報を分割し、分割されたユーザ認証情報の各構成要素のうち、一方の構成要素をシステム側の登録情報、他方の構成要素をユーザ端末２内に設定する登録情報として割当てる。ユーザ認証時に、ユーザ端末２内の登録情報を取得すると共に、ユーザデータベースＤＢからシステム側の登録情報とを取得し、取得したユーザ端末２内の登録情報とシステム側の登録情報とに基づいて元のユーザ認証情報を生成復元した後、復元されたユーザ認証情報と、ユーザ認証時に入力されたユーザ認証情報とを比較してユーザ認証を行う。



認証システム

1

【特許請求の範囲】

【請求項１】ユーザ認証時に入力されたユーザ認証情報と、予め設定登録されているユーザ認証情報とを照合することによってユーザ認証を行う管理センタ装置と、ユーザ所有のユーザ端末とが通信ネットワークを介して接続されてなる認証システムであって、ユーザ認証情報を分割する分割手段と、この分割手段によって分割されたユーザ認証情報の各構成要素のうち、一方の構成要素をシステム側の登録情報として割り当てると共に、他方の構成要素を前記ユーザ端末内に設定する登録情報として割り当てて分割情報割当手段と、ユーザ認証を行う場合に、そのユーザ端末内に設定されている登録情報を取得すると共に、前記システム側に設定されている登録情報とを取得する登録情報取得手段と、この登録情報取得手段によって取得したユーザ端末内の登録情報とシステム側の登録情報とに基づいて元のユーザ認証情報を生成復元する復元手段と、この復元手段によって復元されたユーザ認証情報と、ユーザ認証時に入力されたユーザ認証情報とを比較してユーザ認証を行うユーザ認証手段と、を具備したことを特徴とする認証システム。

【請求項２】複数のユーザに対応してそれらのユーザ認証情報をそれぞれ設定登録する場合において、前記分割手段によって分割されたユーザ認証情報の構成要素をユーザ側の登録情報として当該ユーザ端末内に設定させる際は、その登録情報がシステム側のどの登録情報に対応するかを示す為の識別情報を含めて当該ユーザ端末内に設定させ、ユーザ認証を行う場合に前記登録情報取得手段は、そのユーザ所有のユーザ端末内に設定されている登録情報と共に前記識別情報を取得し、この識別情報に基づいて対応するシステム側の登録情報を取得する、ようにしたことを特徴とする請求項1記載の認証システム。

【請求項３】ユーザ認証を行った後において、前記分割手段は、前回の分割方法とは異なる方法でユーザ認証情報を再分割し、前記分割情報割当手段は、この分割手段によって再分割されたユーザ認証情報の各構成要素のうち、一方の構成要素をシステム側の登録情報として割り当てると共に、他方の構成要素をユーザ端末内に設定するユーザ側の登録情報として割り当てることにより、前回のユーザ側の登録情報とシステム側の登録情報の内容を変更する、ようにしたことを特徴とする請求項1記載の認証システム。

【請求項４】ユーザ認証が行われる毎に、前記分割手段は、ユーザ認証情報の分割位置をランダムに決定すると共に、この決定された分割位置にしたがってユーザ認証情報を再分割する、ようにしたことを特徴とする請求項３記載の認証システム。

【請求項５】ユーザの特徴情報をユーザ認証情報として検知する検知装置を設け、この検知装置とそのユーザ所持の携帯通信装置との間で近距離無線通信を行うと共に、この携帯通信装置は、前記検知装置によって検知されたユーザ認証情報を受信して前記管理センタ装置へ送信し、前記管理センタ装置は、前記携帯通信装置から送信されて来たユーザ認証情報を分割すると共に、分割されたユーザ認証情報の各構成要素のうち、一方の構成要素をシステム側の登録情報として割り当てると共に、他方の構成要素を前記ユーザ端末内に設定する登録情報として割り当てる、ようにしたことを特徴とする請求項1記載の認証システム。

【請求項６】前記分割手段は、ユーザ認証情報を複数の分割位置で分割し、前記分割情報割当手段は、前記複数の分割位置によって細かく分割されたユーザ認証情報の各構成要素のうち、システム側に割り当てるべき構成要素と、ユーザ端末内に割り当てるべき構成要素とを選択決定する、ようにしたことを特徴とする請求項1記載の認証システム。

【請求項７】コンピュータに対して、ユーザ認証情報を分割する機能と、分割されたユーザ認証情報の各構成要素のうち、一方の構成要素をシステム側の登録情報として割り当てると共に、他方の構成要素を前記ユーザ端末内に設定する登録情報として割り当てる機能と、ユーザ認証を行う場合に、そのユーザ端末内に設定されている登録情報を取得すると共に、前記システム側に設定されている登録情報とを取得する機能と、取得したユーザ端末内の登録情報とシステム側の登録情報とに基づいて元のユーザ認証情報を生成復元する機能と、復元されたユーザ認証情報と、ユーザ認証時に入力されたユーザ認証情報とを比較してユーザ認証を行う機能と、を実現させるためのプログラム。

【請求項８】ユーザ認証を行う管理センタ装置と、ユーザ所有のユーザ端末とが通信ネットワークを介して接続されているシステム環境において、ユーザ認証時に入力されたユーザ認証情報と、予め設定登録されているユーザ認証情報とを照合することによってユーザ認証を行う認証方法であって、ユーザ認証情報を分割すると共に、分割されたユーザ認証情報の各構成要素のうち、一方の構成要素をシステム側の登録情報として割り当てると共に、他方の構成要素を前記ユーザ端末内に設定する登録情報として割り当て、ユーザ認証を行う場合に、そのユーザ端末内に設定されている登録情報を取得すると共に、前記システム側に設定されている登録情報とを取得し、取得したユーザ端末内の登録情報とシステム側の登録情報とに基づいて元のユーザ認証情報を生成復元し、復元されたユーザ認証情報と、ユーザ認証時に入力されたユーザ認証情報とを比較してユーザ認証を行う、ようにしたことを特徴とする認証方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】この発明は、ユーザ認証時に入力されたユーザ認証情報と、予め設定登録されている

ユーザ認証情報とを照合することによってユーザ認証を行う認証システム、そのプログラム、認証方法に関する。

【０００２】

【従来の技術】従来、本人確認を行う認証システムとしては、例えば、図１３（ａ）に示すように、センサシステム（指紋センサ）によって検知された指紋パターンデータがインターネットや構内通信網を介してサーバ側のハードディスク内に個人識別情報（ユーザ認証情報）として登録管理されている状態において、ユーザ認証時には、図１３（ｂ）に示すように、センサシステムによって検知された指紋パターンデータと、サーバ側のハードディスク内に設定登録されている指紋パターンデータとを照合し、その照合結果に応じて例えば、コンピュータ装置へのアクセス可否を決定するようにしている。また、独身マンション入室管理システムや建物入館管理システム等においては、本人確認を行う認証システムが備えられており、指紋センサ装置から入力された指紋パターンデータが予めユーザ認証情報として設定登録されている状態において、ユーザ認証時に、指紋センサ装置から指紋パターンデータが入力されると、予め設定登録されているユーザ認証情報（登録情報）と今回入力された指紋パターンデータとを照合することによってユーザ認証を行い、その認証結果に基づいて入室管理や入館管理を行うようにしている。この場合、いずれの認証システムにおいても、登録情報（指紋パターンデータ）は、その対象者である各ユーザ毎にシステム側に一元管理されている。

【０００３】

【発明が解決しようとする課題】しかしながら、この種の認証システムにおいては、第三者が例えば、擬似指を使って指紋パターンデータを入力したものとすると、偶発的にヒットするケースもあり、また、登録情報を何らかの方法で盗用されるケースもある等、その安全性が要望されていた。このことは、指紋認識の場合に限らず、音声認識、顔写真認識、眼球認識、パスワード認識等の場合においても同様であった。

【０００４】この発明の課題は、設定登録用のユーザ認証情報を複数の構成要素に分割して分散管理することで、設定登録用のユーザ認証情報を効果的に保護することができると共に、設定登録用のユーザ認証情報を複数の構成要素に分割して分散管理したとしても、確実なセキュリティ管理を実現できるようにすることである。

【０００５】この発明の手段は、次の通りである。請求項第１記載の発明は、ユーザ認証時に入力されたユーザ認証情報と、予め設定登録されているユーザ認証情報とを照合することによってユーザ認証を行う管理センタ装置と、ユーザ所有のユーザ端末とが通信ネットワークを介して接続されてなる認証システムであって、ユーザ認証情報を分割する分割手段と、この分割手段によって分

割されたユーザ認証情報の各構成要素のうち、一方の構成要素をシステム側の登録情報として割り当てると共に、他方の構成要素を前記ユーザ端末内に設定する登録情報として割り当てる分割情報割当手段と、ユーザ認証を行う場合に、そのユーザ端末内に設定されている登録情報を取得すると共に、前記システム側に設定されている登録情報とを取得する登録情報取得手段と、この登録情報取得手段によって取得したユーザ端末内の登録情報とシステム側の登録情報とに基づいて元のユーザ認証情報を生成復元する復元手段と、この復元手段によって復元されたユーザ認証情報と、ユーザ認証時に入力されたユーザ認証情報とを比較してユーザ認証を行うユーザ認証手段とを具備するものである。したがって、請求項１記載の発明においては、設定登録用のユーザ認証情報を複数の構成要素に分割して分散管理することで、設定登録用のユーザ認証情報を効果的に保護することができると共に、設定登録用のユーザ認証情報を複数の構成要素に分割して分散管理したとしても、確実なセキュリティ管理を実現することができる。

【０００６】なお、この発明は次のようなものであってもよい。複数のユーザに対応してそれらのユーザ認証情報をそれぞれ設定登録する場合において、前記分割手段によって分割されたユーザ認証情報の構成要素をユーザ側の登録情報として当該ユーザ端末内に設定させる際には、このユーザ側の登録情報がシステム側のどの登録情報に対応するかを示す為の識別情報を含めて当該ユーザ側の登録情報を設定させ、ユーザ認証を行う場合に、前記登録情報取得手段は、そのユーザ所有のユーザ端末内に設定されているユーザ側の登録情報と共に前記識別情報を取得し、この識別情報に基づいて対応するシステム側の登録情報を取得する（請求項２記載の発明）。

【０００７】ユーザ認証を行った後において、前記分割手段は、前回の分割方法とは異なる方法でユーザ認証情報を再分割し、前記分割情報割当手段は、この分割手段によって再分割されたユーザ認証情報の各構成要素のうち、一方の構成要素をシステム側の登録情報として割り当てると共に、他方の構成要素をユーザ端末内に設定するユーザ側の登録情報として割り当てることにより、前回のユーザ側の登録情報とシステム側の登録情報の内容を変更する（請求項３記載の発明）。この場合、ユーザ認証が行われる毎に、前記分割手段は、ユーザ認証情報の分割位置をランダムに決定すると共に、この決定された分割位置にしたがってユーザ認証情報を再分割する（請求項４記載の発明）。

【０００８】ユーザの特徴情報をユーザ認証情報として検知する検知装置を設け、この検知装置とユーザ所持の携帯通信装置との間で近距離無線通信を行うと共に、前記携帯通信装置は、前記検知装置によって検知されたユーザ認証情報を受信して前記管理センタ装置へ送信し、前記管理センタ装置は、前記携帯通信装置から送信され

て来たユーザ認証情報を分割すると共に、分割されたユーザ認証情報の各構成要素のうち、一方の構成要素をシステム側の登録情報として割り当てると共に、他方の構成要素を前記ユーザ端末内に設定するユーザ側の登録情報として割り当てる（請求項５記載の発明）。

【０００９】前記分割手段は、ユーザ認証情報を複数の分割位置で分割し、前記分割情報割当手段は、前記複数の分割位置によって細かく分割されたユーザ認証情報の各構成要素のうち、システム側に割り当てるべき構成要素と、ユーザ端末内に割り当てるべき構成要素を選択決定する（請求項６記載の発明）。

【００１０】他の発明は、コンピュータに対して、上述した請求項１記載の発明に示した主要機能を実現させるためのプログラムを提供し（請求項７記載の発明）、また、上述した請求項１記載の発明に示した主要手順にしたがった処理を行う認証方法を提供するものである（請求項８記載の発明）。

【００１１】

【発明の実施の形態】以下、図１～図１１を参照してこの発明の一実施形態を説明する。図１は、この実施形態における認証システムの全体構成を示したブロック図である。この実施形態における認証システムは、マンション入室管理システムに採用したもので、一般参加の募集に応じて参加申込のあった各利用者（マンションの管理者）側との間で利用契約を行って会員登録を行い、その会員マンションの各入居者に対するユーザ認証サービスを代行するサービス事業を全国規模で展開するようにした広域通信システムである。このようなユーザ認証サービスを代行する認証システムは、ユーザ認証サービスを行う認証管理センタ１と、各会員マンションの各入居者（ユーザ）所持のユーザ端末（携帯電話端末）２とがネットワーク網（インターネット）３、移動体通信網４を介して接続されているシステム環境となっている。

【００１２】認証管理センタ１は、このセンタの中核をなす管理サーバ１１と、ユーザデータベースＤＢを管理制御するデータベースサーバ１２と、電子メールを管理制御するメールサーバ１３と、Ｗｅｂサーバ１４等の各種サーバを有し、これらのサーバによってこの認証管理センタ１の全体動作を制御するようにしている。なお、この実施形態においては、例えば、ＴＣＰ／ＩＰ通信プロトコルを利用したＨＴＴＰプロトコル等によって、認証管理センタ１とユーザ端末２との間でデジタル化（パケット化）されたデータの送受信を行うようにしており、また、コード化された制御情報を含むデータによって互いに必要な処理内容を認識しながら連携し合ってデータ処理を行うようにしている。なお、ユーザ端末２は、Ｗｅｂブラウザ機能を備えている。

【００１３】会員マンション側には、指紋センサ装置５が配置されいる。この指紋センサ装置５は、会員登録を行った会員マンションに対し有料にて設置されたもので、会員マンションの各入居者を管理するマンション入室管理システム（図２参照）に接続されている。この指紋センサ装置５は、その会員マンションの各入居者所持のユーザ端末（携帯電話端末）２との間において近距離通信によってデータの送受信を行うようにしている。すなわち、近距離通信手段としては、微弱通信規格のＢｌｕｅｔｏｏｔｈ無線通信や赤外線通信規格のＩｒＤＡ無線通信によって指紋センサ装置５と各入居者所持のユーザ端末２との間でデータの送受信を行うようにしている。この場合、認証管理センタ１と指紋センサ装置５とは、ユーザ端末２および広域通信網（インターネット３、移動体通信網４）を介してデータの送受信を行うようにしている。

【００１４】図２は、指紋センサ装置５の全体構成を示したブロック図である。指紋センサ装置５は、指の指紋を検知する光センサ（エリアセンサ）５－１を有し、このエリアセンサ５－１からの検知信号は、フィルタ５－２、サンプリングホールド部５－３を介してＡ／Ｄ変換部５－４に与えられ、Ａ／Ｄ変換部５－４によって変換されたデジタルデータは、特徴抽出部５－５によってユーザ固有の指紋パターンデータに変換され、バッファ５－６を介して近距離無線送信部５－７からユーザ端末２へ送信される。

【００１５】また、指紋センサ装置５には、ユーザ端末２から近距離無線通信によって送信されて来たデータを受信する近距離無線受信部５－８が設けられており、この近距離無線受信部５－８によって受信したデータは、バッファ５－９を介して認証結果判定部５－１０に与えられる。認証結果判定部５－１０は、認証管理センタ１からユーザ端末２を介して送信されて来た認証結果を判別し、認証ＮＧ（否定）、認証ＯＫ（肯定）に応じた判定信号を生成出力するもので、この判定信号はマンション入室管理システム６に送信される。なお、マンション入室管理システム６は、会員マンションである各入居者の入室状況を管理する通常の管理システムである。

【００１６】図３（Ａ）は、ユーザデータベースＤＢの内容を示した図である。このユーザデータベースＤＢは、会員マンションの各入居者に対応して、「氏名」、「連絡先」、「ユーザＩＤ」、「分割登録パターン」、「復元キー」等の各項目を有するユーザレコードを記憶管理する構成となっている。「氏名」は入居者の氏名、「連絡先」は入居者の電話番号や電子メールアドレスであり、「ユーザＩＤ」は、ユーザ登録時に認証管理センタ１側から割り当てられたユーザ固有の識別情報である。

【００１７】また、「分割登録パターン」は、ユーザ認証用として予め設定登録されるユーザ認証情報（指紋パターンデータ）を分割した各構成要素のうち、その一方の構成要素パターンである。すなわち、この実施形態においては、ユーザ認証用として設定登録されるユーザ認

証情報（指紋パターンデータ）を２分割して分散管理するようにしており、その一方の構成要素パターンをシステム側の登録情報として割り当てると共に、他方の構成要素パターンをユーザ側の登録情報として割り当てて設定登録するようにしている。この場合、ユーザデータベースＤＢ内の「分割登録パターン」は、上述したシステム側の登録情報である。

【００１８】「復元キー」は、ユーザ側の登録情報とシステム側の登録情報とに基づいて元のユーザ認証情報を合成復元する際に使用する為の復元用の情報であり、この実施形態においては、設定登録用のユーザ認証情報を分割した分割位置を示す情報である。この実施形態においては、ユーザ認証情報（指紋パターンデータ）を２分割する場合、その分割位置を「復元キー」として登録しておき、復元時にはこの「復元キー」によって示される分割位置にしたがってユーザ側の登録情報とシステム側の登録情報とを合成復元するようにしている。

【００１９】図３（Ｂ）は、ユーザ認証情報（指紋パターンデータ）を２分割することによって得られた他方の構成要素パターンがユーザ側の登録情報として記憶管理されている状態を示した図である。ここで、「ユーザ登録済みフラグ」は、ユーザ側の登録情報がそのユーザ端末２内に登録済みであることを示すフラグである。また、ユーザ側の登録情報は、「分割登録パターン」に「ユーザＩＤ」を付加してユーザ端末２内のメモリに記憶管理されている。

【００２０】図４は、ユーザ端末２から認証管理センタ１へ送信される伝送フォーマットを示したもので、（Ａ）は、ユーザ登録時の伝送フォーマット、（Ｂ）はユーザ認証時の伝送フォーマットを示している。ユーザ登録時の伝送フォーマットは、「ヘッダー」、「登録」、「レングスＬ」、「指紋パターンデータ」、「ユーザＩＤ」の各データからなり、「指紋パターンデータ」は、設定登録用のユーザ認証情報であり、「レングスＬ」は「指紋パターンデータ」のデータ長を示している。ユーザ認証時の伝送フォーマットは、「ヘッダー」、「認証」、「今回入力の指紋パターンデータ」、「ユーザ既登録パターン」、「ユーザＩＤ」の各データからなり、「ユーザ既登録パターン」は、上述したユーザ側の登録情報である「分割登録パターン」であり、「今回入力の指紋パターンデータ」は、ユーザ認証時に検知されたデータである。

【００２１】図５は、認証管理センタ１の中核を成す管理サーバ１１の全体構成を示したブロック図である。ＣＰＵ１１１は、記憶装置１１２内のオペレーティングシステムや各種アプリケーションソフトにしたがってこの管理サーバ１１の全体動作を制御する中央演算処理装置である。記憶装置１１２は、オペレーティングシステムや各種アプリケーションソフト等が格納され、磁気的、光学的、半導体メモリ等によって構成されている記録媒体１１３やその駆動系を有している。この記録媒体１１３はハードディスク等の固定的な媒体若しくは着脱自在に装着可能なＣＤ－ＲＯＭ、フロッピィデスク、ＲＡＭカード、磁気カード等の可搬型の媒体である。また、この記録媒体１１３内のプログラムやデータは、必要に応じてＣＰＵ１１１の制御によりＲＡＭ（例えば、スタティックＲＡＭ）１１４にロードされたり、ＲＡＭ１１４内のデータが記録媒体１１３にセーブされる。更に、記録媒体は外部機器側に設けられているものであってもよく、ＣＰＵ１１１は伝送制御部１１５を介してこの記録媒体内のプログラム／データを直接アクセスして使用することもできる。

【００２２】また、ＣＰＵ１１１は記録媒体１１３内に格納されるその一部あるいは全部を他の機器側から伝送制御部１１５を介して取り込み、記録媒体１１３に新規登録あるいは追加登録することもできる。更に、プログラム／データはサーバ等の外部機器側で記憶管理されているものであってもよく、ＣＰＵ１１１は伝送制御部１１５を介して外部機器側のプログラム／データを直接アクセスして使用することもできる。一方、ＣＰＵ１１１にはその入出力周辺デバイスである伝送制御部１１５、入力部１１６、表示部１１７がバスラインを介して接続されており、入出力プログラムにしたがってＣＰＵ１１１はそれらの動作を制御する。

【００２３】図６は、ユーザ端末２の全体構成を示したブロック図である。なお、ユーザ端末２の構成要素も上述した管理サーバ１１の構成要素に対応して、ＣＰＵ２０１、記憶装置２０２、ＲＡＭ２０３、入力部２０４、表示部２０５の他、近距離無線通信部２０６、広域無線通信部２０７を有する構成となっている。近距離無線通信部２０６は、指紋センサ装置５との間でＢｌｕｅｔｏｏｔｈ無線通信やＩｒＤＡ無線通信によってデータの送受信を行うものであり、広域無線通信部２０７は、認証管理センタ１との間でインターネット３、移動体通信網４を介してデータの送受信を行うものである。

【００２４】次に、この実施形態における認証システムの動作アルゴリズムを図７～図１０に示すフローチャートを参照して説明する。ここで、これらのフローチャートに記述されている各機能、つまり、図７に記述したユーザ登録処理、図８および図９に記述したユーザ認証処理、図１０に記述したユーザ端末側の処理は、読み取り可能なプログラムコードの形態で格納されており、認証管理センタ１やユーザ端末２は、このプログラムコードにしたがった動作を逐次実行する。また、伝送媒体を介して伝送されてきた上述のプログラムコードにしたがった動作を逐次実行することもできる。すなわち、記録媒体の他、伝送媒体を介して外部供給されたプログラム／データを利用してこの実施形態特有の動作を実行することもできる。

【００２５】図７～図９は、認証管理センタ１側におい

て実行される動作を示したフローチャートであり、図１０は、ユーザ端末２側の主要動作（この実施形態固有の動作）を示したフローチャートである。先ず、認証管理センタ１側でのユーザ登録処理と、この登録処理に応答して実行されるユーザ端末２側での動作を説明する。いま、登録会員であるマンションの入居者であるユーザは、自己のユーザ端末２から認証管理センタ１に対してユーザ登録要求を行うが、この場合、「ユーザ登録済みフラグ」を参照し、「ユーザ登録済みフラグ」がオンされているかをチェックし（図１０のステップＤ１）、当該フラグがオフされていることを条件にユーザ登録指示を受け付け（ステップＤ２）、認証管理センタ１に対してユーザ登録要求を行う（ステップＤ３）。

【００２６】認証管理センタ１は、ユーザからの登録アクセス待ち状態において（図７のステップＡ１）、いずれかのユーザ端末２から登録要求を受信すると、ユーザ登録入力ページを要求元のユーザ端末２へ送信する（ステップＡ２）。ユーザ端末２は、このユーザ登録入力ページを受信すると（図１０のステップＤ４）、その入力ページ画面を表示出力させる（ステップＤ５）。このユーザ登録入力ページ画面は、「登録会員マンション名」の他に、そのの入居者の「氏名」、「連絡先」等の各項目に対応してその入力領域を有するもので、このページ画面内に必要事項を入力した後、当該ページ画面内の送信ボタンを操作すると、入力されたユーザ情報は、認証管理センタ１へ送信される（ステップＤ６）。

【００２７】認証管理センタ１は、ユーザ情報を受信すると（図７のステップＡ３）、そのユーザに割り当てるべきユーザＩＤを発行して要求元のユーザ端末２へ送信する（図７のステップＡ４）。この場合、ユーザ端末２は、認証管理センタ１から送信されて来たユーザＩＤを受信して登録する（図１０のステップＤ７）。そして、認証管理センタ１は、受信したユーザ情報をユーザデータベースＤＢに追加登録した後（図７のステップＡ５）、要求元のユーザ端末２へ指紋パターンデータの入力を促す為のメッセージを含む指紋入力通知を行う（ステップＡ６）。

【００２８】ユーザ端末２は、指紋入力通知を受信すると、そのメッセージ内容を表示出力してユーザに報知する（図１０のステップＤ８）。ここで、ユーザは、指紋センサ装置５のエリアセンサ５－１上に指を載せると、フィルタ５－２、サンプリングホールド部５－３、Ａ／Ｄ変換部５－４、特徴抽出部５－５、バッファ５－６、近距離無線送信部５－７を介してユーザ端末２へ指紋パターンデータが送信される。ユーザ端末２は、指紋センサ装置５によって検知された指紋パターンデータを受信すると（図１０のステップＤ９）、図４（Ａ）に示したような登録伝送フォーマットに、「指紋パターンデータ」、「データ長Ｌ」、「ユーザＩＤ」等を配置した伝送データを作成して認証管理センタ１へ送信する（ステップＤ１０）。その後、「ユーザ登録済みフラグ」をオンさせる（ステップＤ１１）。

【００２９】認証管理センタ１は、ユーザ端末２から送信されて来た登録伝送データを受信すると（図７のステップＡ７）、「指紋パターンデータ」、「データ長Ｌ」を抽出し、この「データ長Ｌ」にしたがって「指紋パターンデータ」の中点を求め、この中点を境に「指紋パターンデータ」を２分割する（ステップＡ８）。図１１（Ａ）は、この場合の分割状態を示した図で、その前半部の分割パターンがシステム側の登録情報となり、後半部の分割パターンがユーザ側の登録情報となる。

【００３０】そして、前半部の分割パターン（システム側の登録情報）を「ユーザＩＤ」と共にユーザデータベースＤＢに登録する他（ステップＡ９）、「復元キー」を生成してユーザデータベースＤＢの該当項目に登録する（ステップＡ１０）。この場合の「復元キー」は、中点位置情報となる。また、後半部の分割パターンをユーザ側の登録情報として、その「ユーザＩＤ」と共に、要求元のユーザ端末２へ送信する（ステップＡ１１）。

【００３１】ユーザ端末２は、「ユーザ登録済みフラグ」がオンされている状態において（図１０のステップＤ１）、認証管理センタ１からその「ユーザＩＤ」と共に送信されて来た分割パターン（ユーザ側の登録情報）を受信すると（ステップＤ１２）、受信した「ユーザＩＤ」と予め登録されている自己の「ユーザＩＤ」とが一致するかを判別し（ステップＤ１３）、不一致の場合には、受信データを無視するが、一致する場合には、受信した分割パターン（後半部）を登録する処理を行う（ステップＤ１４）。

【００３２】図８および図９は、認証管理センタ１側で実行されるユーザ認証処理を示したフローチャートである。以下、認証管理センタ１側でのユーザ認証処理と、この認証処理に応答して実行されるユーザ端末２側での動作を図１０に示すフローチャートを参照して説明する。先ず、ユーザ認証時において、ユーザは指紋センサ装置５に指を載せると、この指紋センサ装置５によって検知された指紋パターンデータは、ユーザ端末２へ送信される。ユーザ端末２は、指紋センサ装置５からの指紋パターンデータを受信すると（図１０のステップＤ１５）、ユーザ側の登録情報である「ユーザ登録分割パターン」と「ユーザＩＤ」とを取得し（ステップＤ１６）、図４（Ｂ）に示したような認証用の伝送フォーマットに、「今回入力の指紋パターンデータ」、「ユーザ登録分割パターン」、「ユーザＩＤ」等を配置した伝送データを作成して認証管理センタ１へ送信する（ステップＤ１７）。

【００３３】認証管理センタ１は、この認証アクセス要求を受信すると（図８のステップＢ１）、この受信データの中から「今回入力の指紋パターンデータ」、「ユーザ登録分割パターン」、「ユーザＩＤ」を抽出し（ステ

ップＢ２）、この「ユーザＩＤ」に基づいてユーザデータベースＤＢを検索し（ステップＢ３）、それに該当するシステム側の「登録分割パターン」が有るかを判別し（ステップＢ４）、無ければ、認証ＮＧ（否定）を要求元のユーザ端末２へ送信するが（ステップＢ１１）、有れば、該当するシステム側の「登録分割パターン」と「復元キー」とをユーザデータベースＤＢから取得する（ステップＢ５）。そして、この「復元キー」に基づいてパターン展開用の座標系上の合成位置を求め、この位置を基準として、「システム側登録分割パターン」と「ユーザ側登録分割パターン」とを配置して元の「指紋パターンデータ」を合成復元する（ステップＢ６）。

【００３４】そして、認証管理センタ１は、復元した「指紋パターンデータ」と「今回入力の指紋パターンデータ」とを比較し（ステップＢ７）、両者の一致を判別する（ステップＢ８）。ここで、不一致の場合には、認証ＮＧ（否定）を要求元のユーザ端末２へ送信するが（ステップＢ１１）、一致する場合には、認証ＯＫ（肯定）を要求元のユーザ端末２へ送信する（ステップＢ９）。この場合、ユーザ端末２では、認証管理センタ１からの認証結果を受信すると（図１０のステップＤ１８）、その受信結果を表示出力すると共に（ステップＤ１９）、指紋センサ装置５へその認証結果を送信する（ステップＤ２０）。

【００３５】指紋センサ装置５において、その近距離無線受信部５－８によって受信したデータがバッファ５－９を介して認証結果判定部５－１０に与えられると、認証結果判定部５－１０は、認証管理センタ１からユーザ端末２を介して送信されて来た認証結果を判別し、認証ＮＧ（否定）、認証ＯＫ（肯定）に応じた判定信号を生成出力してマンション入室管理システム６に送信される。

【００３６】その後、認証管理センタ１は、認証ＯＫ（肯定）の場合には（図８のステップＢ８）、指紋パターン再登録処理に移る（ステップＢ１０）。図９は、この指紋パターン再登録処理を示したフローチャートである。認証管理センタ１は、乱数発生器（図示せず）からランダム数値を取得し（ステップＣ１）、このランダム数値に基づいて分割位置を決定する（ステップＣ２）。例えば、数値“１”～“２０”の中から発生されたランダム数値に対応付けられている分割位置を今回の分割位置として決定する。そして、上述のようにして復元された「指紋パターンデータ」を決定位置で再分割する（ステップＣ３）。

【００３７】図１１（Ｂ）は、ランダム分割された状態を例示した図で、その前部の分割パターンがシステム側の登録情報となり、後部の分割パターンがユーザ側の登録情報となることは、上述の場合と同様であるが、（Ａ）の場合に比べて、ランダム分割によってその分割位置が異なっている。この場合、システム側の方がユーザ側よりもそのデータ長は大きくなっている。なお、（Ｃ）は、次の指紋パターン再登録処理によって分割された状態を例示した図で、更に、その分割位置は異なり、ユーザ側の方がシステム側よりもそのデータ長は大きくなっている。

【００３８】そして、認証管理センタ１は、ランダム分割による「復元キー」を生成してユーザデータベースＤＢの該当項目に登録することによってその内容を変更すると共に（ステップＣ４）、ランダム分割によって得られた前部の分割パターンをシステム側の登録情報として、ユーザデータベースＤＢの該当項目に登録することにより前回の内容を変更する（ステップＣ５）。そして、後部の分割パターンをユーザ側の登録情報として、要求元のユーザ端末２へ送信する（ステップＣ６）。すると、ユーザ端末２側では、認証管理センタ１から送信されて来たユーザ登録用の分割パターンを受信すると（図１０のステップＤ１２）、その「ユーザＩＤ」が一致することを条件に（ステップＤ１３）、当該分割パターンを登録することにより、前回の内容を変更する（ステップＤ１４）。

【００３９】以上のように、この実施形態において認証管理センタ１は、ユーザ登録時に、指紋センサ装置５からユーザ端末２を介して通信されて来たユーザ認証情報（指紋パターンデータ）を分割すると共に、分割されたユーザ認証情報の各構成要素のうち、一方の構成要素をシステム側の登録情報として割り当てると共に、他方の構成要素をユーザ側の登録情報として割り当てて設定登録させるようにしたから、設定登録用のユーザ認証情報を複数の構成要素に分割して分散管理することができる。したがって、例えば、ユーザ端末２内に設定されているユーザ側の登録情報が盗用されたとしても、それは登録情報の一部だけである為にセキュリティ上、問題となることはなく、登録情報を効果的に保護することが可能となる。

【００４０】この場合、ユーザ認証時において認証管理センタ１は、当該ユーザ端末２に設定されているユーザ側の登録情報を取得すると共に、認証管理センタ１のユーザデータベースＤＢに設定されているシステム側の登録情報とを取得し、取得したユーザ側の登録情報とシステム側の登録情報とに基づいて元のユーザ認証情報を生成復元した後、復元されたユーザ認証情報と、ユーザ認証時に入力されたユーザ認証情報とを比較してユーザ認証を行うようにしたから、設定登録用のユーザ認証情報を複数に分割して分散管理したとしても、ユーザ認証を確実に行うことが可能となる。

【００４１】また、複数のユーザに対応してそれらのユーザ認証情報をそれぞれ設定登録する場合において、認証管理センタ１は、分割したユーザ認証情報の構成要素をユーザ側の登録情報としてユーザ端末２に設定登録させる際に、このユーザ側の登録情報がシステム側のどの

登録情報に対応するかを示す為の識別情報（ユーザＩＤ）を含めてそのユーザ側の登録情報を設定し、ユーザ認証を行う場合には、そのユーザ端末２に設定されているユーザ側の登録情報と共にユーザＩＤを取得し、このユーザＩＤに基づいて対応するシステム側の登録情報を取得して復元処理を行うようにしたから、複数ユーザに対応してそれらの登録情報を分散管理したとしても、ユーザ別ユーザ認証を確実に行うことが可能となる。

【００４２】また、ユーザ認証を行った後において、認証管理センタ１は、前回の分割方法とは異なる方法でユーザ認証情報を再分割するようにしたから、分散管理される登録情報をユーザ認証毎に変更することができ、盗用等から登録情報を効果的に保護することができる。この場合、ユーザ認証情報の分割位置をランダムに決定し、その分割位置にしたがって再分割するようにしたから、より確実な保護が可能となる。

【００４３】また、ユーザの特徴情報である指紋を検知する指紋センサ装置５と、そのユーザ所持の携帯電話（ユーザ端末２）との間で近距離無線通信を行うようにしたから、つまり、本人だけが所持する携帯電話を介して指紋センサ装置５と認証管理センタ１との間でデータの送受信を行うようにしたから、第三者が介入する余地が無くなり、また、携帯電話を紛失したり、盗難されたとしても、携帯電話に設定されている登録情報は、その一部であるために安全性を確保することができる。

【００４４】なお、上述した実施形態においては、ユーザ認証情報を２分割する場合を示したが、図１２に示すように、３分割するようにしてもよく、分割数は任意である。この場合、ユーザ認証情報を複数の分割位置で分割し、この複数位置によって細かく分割されたユーザ認証情報の各構成要素のうち、システム側に割り当てるべき構成要素と、ユーザ側に割り当てるべき構成要素を任意に選択して決定するようにしてもよい。例えば、システム側に割り当てるべき構成要素とユーザ側に割り当てるべき構成要素とを交互に決定したり、任意に選択して決定して分散管理させるようにしてもよい。

【００４５】また、上述した実施形態における認証システムは、マンション入室管理システム６に連動するようにしたが、これに限らず、パーソナルコンピュータをオープンする際に、ユーザ認証を行ってアクセス可否を制御する者であってもよい。また、ユーザ認証情報としては、指紋パターンデータに限らず、音声認識、顔写真認識、眼球認識、パスワード認識等をユーザ認証情報としてもよい。更に、ユーザ個人の認証に限らず、グループ認証等であってもよい。

【００４６】一方、コンピュータ（認証管理センタ１）に対して、上述した各手段を実行させるためのプログラムコードをそれぞれ記録した記録媒体（例えば、ＣＤ－ＲＯＭ、フロッピィディスク、ＲＡＭカード等）を提供するようにしてもよい。すなわち、コンピュータが読み取り可能なプログラムコードを有する記録媒体であって、ユーザ認証情報を分割する機能と、分割されたユーザ認証情報の各構成要素のうち、一方の構成要素をシステム側の登録情報とすると共に、他方の構成要素をユーザ側の登録情報として設定する機能と、ユーザ認証を行う場合に、当該ユーザ端末に設定されているユーザ側の登録情報を取得すると共に、前記システム側に設定されているシステム側の登録情報とを取得する機能と、取得したユーザ側の登録情報とシステム側の登録情報とに基づいて元のユーザ認証情報を生成復元する機能と、復元されたユーザ認証情報と、ユーザ認証時に入力されたユーザ認証情報とを比較してユーザ認証を行う機能とを実現させるためのプログラムを記録したコンピュータが読み取り可能な記録媒体を提供するようにしてもよい。

【００４７】

【発明の効果】この発明によれば、ユーザ登録時に、ユーザ端末を介して通信されて来たユーザ認証情報を分割すると共に、分割されたユーザ認証情報の各構成要素のうち、一方の構成要素をシステム側の登録情報とすると共に、他方の構成要素をユーザ側の登録情報として設定させるようにしたから、設定登録用のユーザ認証情報を複数の構成要素に分割して分散管理することができる。したがって、例えば、ユーザ端末に設定されているユーザ側の登録情報が盗用されたとしても、それは登録情報の一部だけである為にセキュリティ上、問題となることはなく、登録情報を効果的に保護することが可能となる。この場合、ユーザ認証時においてユーザ端末に設定されているユーザ側の登録情報を取得すると共に、システム側の登録情報とを取得し、取得したユーザ側の登録情報とシステム側の登録情報とに基づいて元のユーザ認証情報を生成復元した後、復元されたユーザ認証情報と、ユーザ認証時に入力されたユーザ認証情報とを比較してユーザ認証を行うようにしたから、設定登録用のユーザ認証情報を複数に分割して分散管理したとしても、ユーザ認証を確実に行うことが可能となる。

【図面の簡単な説明】

【図１】認証システムの全体構成を示したブロック図。

【図２】指紋センサ装置５の全体構成を示したブロック図。

【図３】（Ａ）は、ユーザデータベースＤＢの内容を示した図、（Ｂ）は、ユーザ認証情報（指紋パターンデータ）を２分割することによって得られた他方の構成要素パターンがユーザ側の登録情報として記憶管理されている状態を示した図。

【図4】ユーザ端末２から認証管理センタ１へ送信される伝送フォーマットを示し、（Ａ）は、ユーザ登録時の伝送フォーマット、（Ｂ）はユーザ認証時の伝送フォーマットを示した図。

【図５】認証管理センタ１の中核を成す管理サーバ１１の全体構成を示したブロック図。

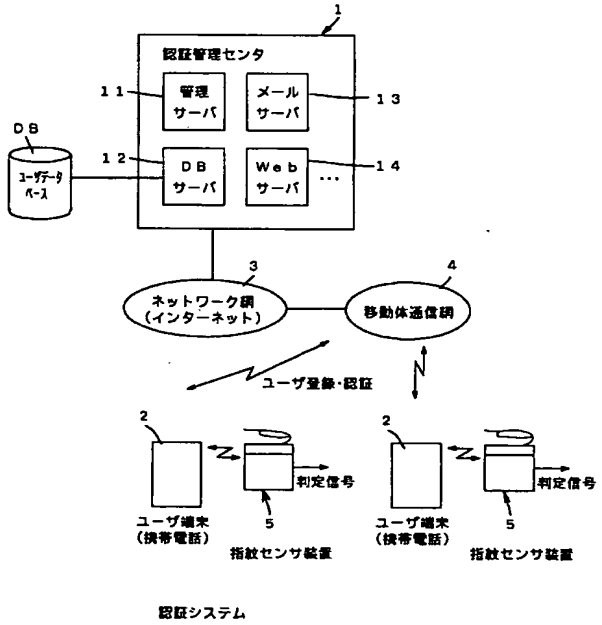
15

【図6】ユーザ端末２の全体構成を示したブロック図。
【図７】認証管理センタ１側において実行されるユーザ登録処理を示したフローチャート。
【図８】認証管理センタ１側で実行されるユーザ認証処理を示したフローチャート。
【図９】上述のユーザ認証処理において実行される指紋パターン再登録処理を示したフローチャート。
【図１０】ユーザ端末２側の主要動作（この実施形態固有の動作）を示したフローチャート。
【図１１】（Ａ）は、ユーザ登録時における指紋パターンデータの分割状態を示した図、（Ｂ）は、指紋パターン再登録処理によってランダム分割された指紋パターンデータの分割状態を例示した図、（Ｃ）は、次の指紋パターン再登録処理によってランダム分割された状態を例示した図。
【図１２】指紋パターンデータを分割して登録する場合の変形応用例を示した図。
【図1-3】（a）、（b）は、従来例を説明する為の図。
【符号の説明】

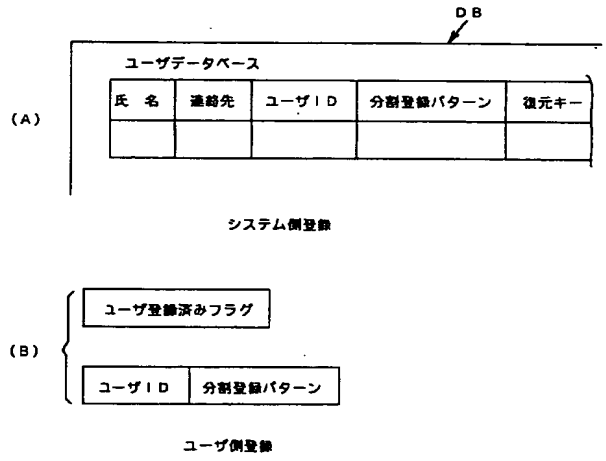
16

１　認証管理センタ
２　ユーザ端末
３　ネットワーク網
４　移動体通信網
５　指紋センサ装置
６　マンション入室管理システム
１１　管理サーバ
１２　データベースサーバ
１３　メールサーバ
１４　Ｗｅｂサーバ
５－７　近距離無線送信部
５－８　近距離無線受信部
５－１０　認証結果判定部
ＤＢ　ユーザデータベース
１１１、２０１　ＣＰＵ
１１２、２０２　記憶装置
１１３　記録媒体
１１５　伝送制御部
２０６　近距離無線通信部
２０７　広域無線通信部

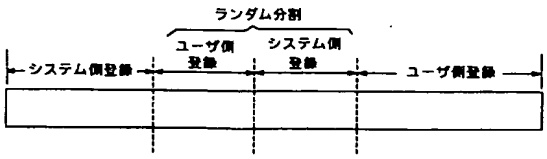
【図１】



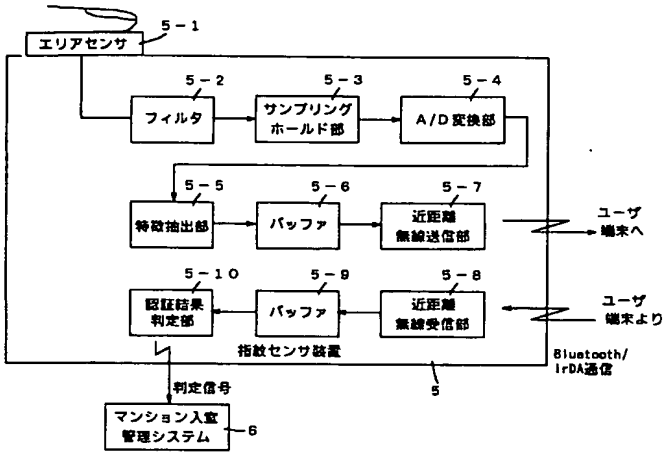
【図３】



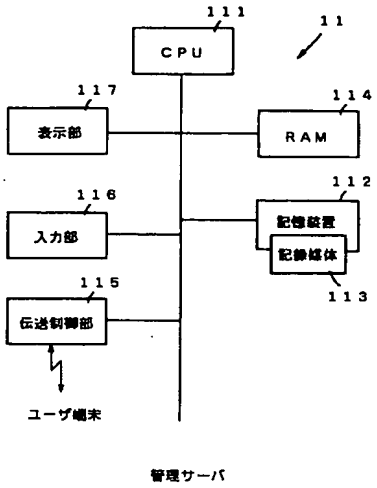
【図１２】



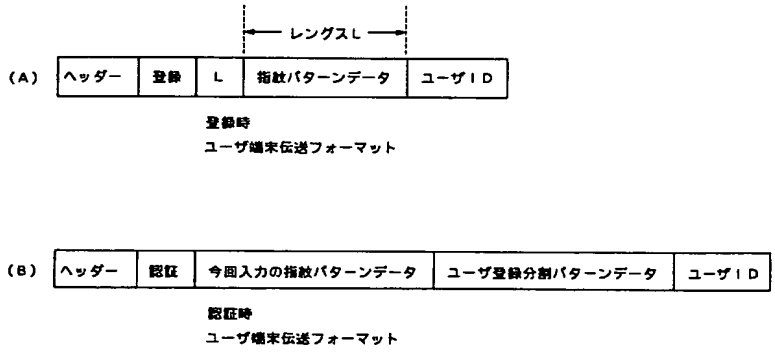
【図２】



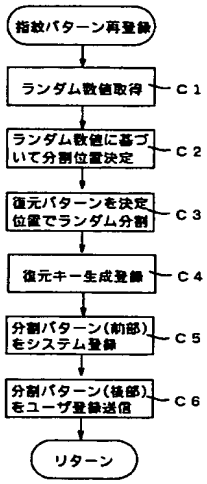
【図５】



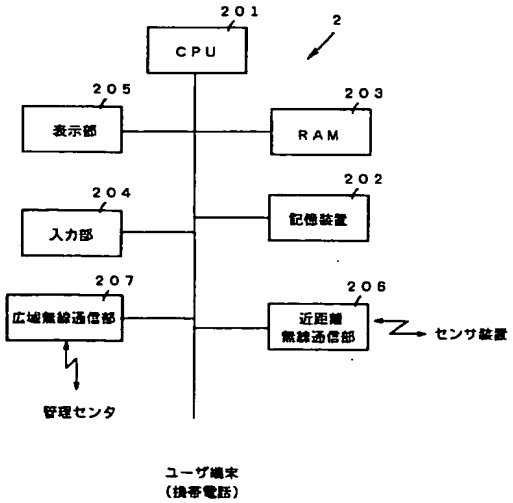
【図４】



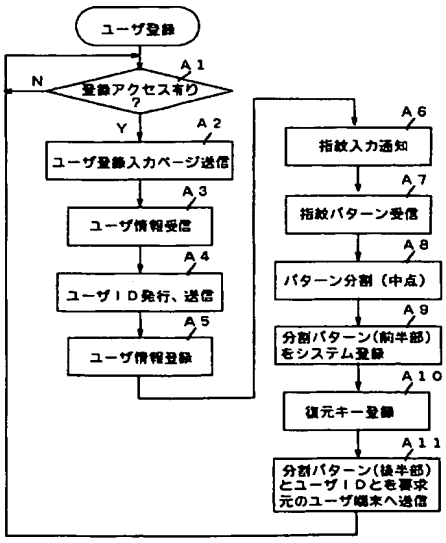
【図９】



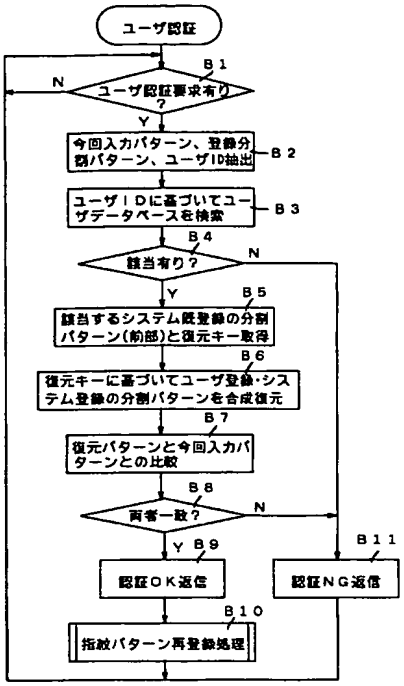
【図６】



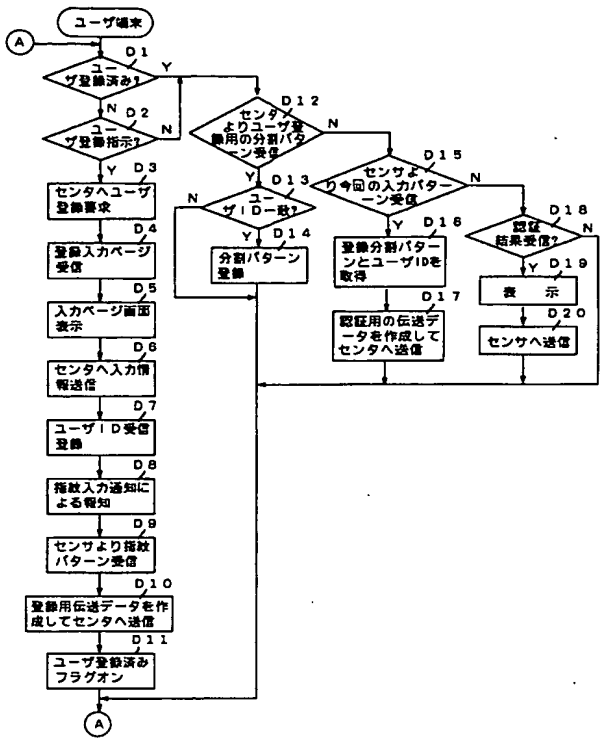
【図７】



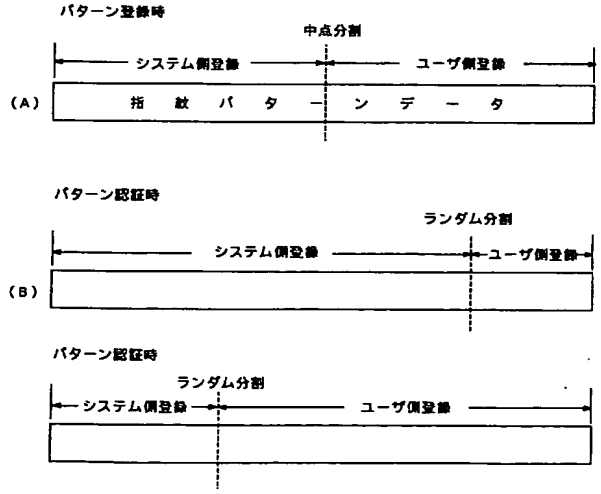
【図８】



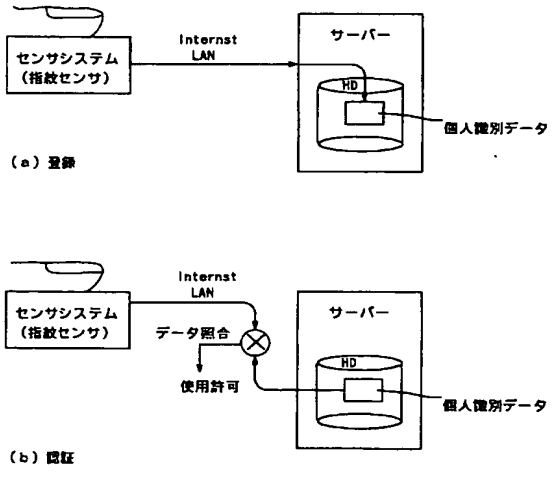
【図１０】



【図１１】



【図１３】



フロントページの続き

(51)Int.Cl.[7]	識別記号	ＦＩ	ﾃｰﾏｺｰﾄﾞ(参考)
		Ｈ０４Ｌ　9/00	６０１Ｄ